SOPHTLOGIC

Who Can See What - WCSW Setup

User Manual

For more information:
E: diane.mcgovern@sophtlogic.com
T: 01473 255552

Introduction

This is the set up to restrict the view of users to the Duty Rota Book and the Personal Record Card. This is done by creating a privilege profile and setting the 'Data Role' to the appropriate level, so that users can see personnel within their location, department, watch system. Etc.

Setup - SOPHT.vault

Initially the SOPHT.vault must be set up. This is done by a SOPHTLOGIC engineer.

TUI Accounts

Every user must have a Trusted User Interface record (TUI). These were all popuklated by Sophtlogic for all current personnel but new personnel will need setting up and deleting when leaving. When personnel change posting this process is automated using a parameter.

The TUI Account is either maintained via 1. File>SOPHT.vault>Setup>TUI Accounts or 2. PRC.

1. Click the green tick to see all entries currently set up. Click the 'Add' button.

Cipher ID	Firstname.lastname (NOTE: if we want pass through this will need to match active directory()
Cipher Number	FIRSTNAME.LASTNAME
Effective From	Date effective from
Expires As At	expiry date
Parent Domain	select FRS name from list (contact SOPHTLOGIC if nothing to select)

Click OK.

2. It is also possible to setup the same information via the Personnel Record Card >TUI Accounts, which is easier to do.

Parameters

Parameters are usually setup by SOPHTLOGIC. There needs to be one parameter for each user.

File > Configuration > System Setup > Parameters

Q0370000.f_param.personnel_wcw_enabled

This must be set to yes with each username in the bottom box. It is possible to duplicate and just change the username.

gate.f_param.tui_auto_update_passport_dbc

This parameter needs to be set to yes. This will set the system to automatically update the TUI Account against a person when a posting amendment is carried that affects the TUI (e.g. change of post).

Privilage Profile

Once the personnel_wcw_enabled has been set, when users log in the system will determine which other personnel the user can see. This is achieved by setting the 'Data Role' of the privilege profile to the appropriate level.

File>Administration>Access Manager>Privilege Profiles>Add/Amend

Description:	**Descri ption of profile, e.g. Station user**	
Team Scope:	Data Class:	Personnel
	Data Role:	Select as per following: **Organisation** – user can see all other users Command – All users in the same division as the user **Location** – all users in the same location as the user **Rota** – all users with the same rota only **Post** – all users with the same post only **Duty System Type** – all users with the same type of duty system (APTC, Control etc) **Post Zone** – all users in posts in the same post zone
Personnel data Restrictions	Ignore	
Enabled	Check the box	

If a user is a member of more than one privilege profile the system will use the highest level Data Role. For instance if one profile is set to Organisation and one to Command then the user will see across the organisation.

So the steps are:

1. Set up the username and password
2. Add or amend the TUI
3. Add the personnel_wcw_enabled parameter
4. Add the user to a privilege profile